REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application, and for withdrawing the claim rejections over the Advanced Encryption Standard (AES) as disclosed by the Stein et al. published patent application.

The independent claims have been amended to more clearly define the claimed invention over the cited prior art references. Support for the claim amendments is best illustrated in FIG. 2, where the first signals **25a-25n** from the input stage **22** are in parallel, as well as the substitution units **27a-27n** in the intermediate stage **24** operating in parallel. The claim arguments and arguments supporting patentability of the claims are provided below.

I. The Amended Claims

The present invention, as recited in amended independent Claim 1, for example, is directed to a cryptographic device comprising an input stage, and an intermediate stage connected to the input stage. The input stage receives an input data block and a key data block comprising a plurality of sub-key data blocks, and generates a plurality of first signals therefrom that are in parallel. The intermediate stage comprises a plurality of substitution units operating in parallel, each substituting data within a respective first signal. A diffuser is connected to the plurality of substitution units for mixing data to generate a diffused signal. An output stage is connected to the intermediate stage for repetitively looping back the

diffused signal to the input stage for combination with a next sub-key data block.

Amended independent Claim 10 is directed to a communication system comprising a key scheduler and a cryptographic device connected to the key scheduler, and has been amended similar to independent Claim 1.

Amended independent Claim 18 is directed to a method for converting an input data block into an output signal in a cryptographic device, and has been amended similar to independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 10 and 18 over the Published Patent Application to Luyster. Luyster is directed to a block cipher secret-key cryptographic system that uses data-dependent rotations and variable rotations of data in block cipher rounds that are dependent, directly or indirectly, on plain text data being enciphered. The Examiner has taken the position that the data encryption system in Luyster discloses every feature of the independent claims.

The data encryption system in Luyster encrypts an n-bit block of input in a plurality of rounds. The data encryption system includes a computing unit for the execution of each round; memory for storing and loading segments; a bit-moving function capable of rotating, shifting, or bit-permute round segments by predetermined numbers of bits to achieve active and effective fixed rotation; a linear combination function which provides new one-to-one round segments using a round operator generally from

one algebraic group to combine two different one-to-one round segments taken from one one-to-one round segment set; and a nonlinear function which affects a one-to-one round segment from a particular one-to-one round segment set based on a value which depends on a preselected number of bits in a preselected location from a different one-to-one round segment from the same one-to-one round segment set. The nonlinear function is a variable rotation function or an s-box. A sub-key combining function is generally employed in each round to provide new round segments by combining a round.

The Applicants submit that the Luyster patent application fails to disclose the claimed invention. As best illustrated in FIG. 7 of Luyster, the substitution units **158** and **170** are not operating in parallel as in the claimed invention. Instead, the substitution units **158, 170** are positioned so that they are part of a serial or sequential iterative process. For example, the output of substitution unit **158** feeds to the input of substitution unit **170**, which is downstream from substitution unit **158**.

This iterative process continues for each round. Reference is directed to page 24, column 285 of Luyster, which provides:

> "Prior to beginning the iterative process, the method shown in FIG. 7 takes the right primary round segment **R1** and linearly combines (block **156**) it using operator **L1** with a subkey segment **K1**. Next, the first of a plurality of rounds of encryption

> (preferably equal to or exceeding 5 rounds) are performed. Each round of encryption computes new values of the one-to-one primary round segments **R0** and **R1**. Each computation of the two primary segments is similar in form, even though it has different inputs and outputs and uses different registers." (Emphasis added).

In the claimed invention, the plurality of substitution units operate in parallel, each substituting data within a respective first signal. Independent Claim 1 further recites that the plurality of first signals from the input stage are in parallel. Since the input signals are in parallel, each substitution unit is able to substitute data within a respective first signal.

In Luyster, the illustrated first signals become part of the iterative process within the rounds. As a result, substitution unit **158** substitutes data within a respective first signal, but the first signal received by the second substitution unit **170** has been modified with the first signal initially provided for the first substitution unit **158**.

Accordingly, it is submitted that amended independent Claim 1 is patentable over Luyster. Amended independent Claims 10 and 18 are similar to amended independent Claim 1. Therefore, it is submitted that these claims are also patentable over Luyster.

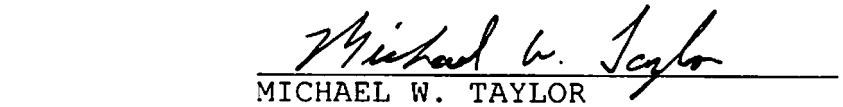
In view of the patentability of amended independent Claims 1, 10 and 18, it is submitted that the dependent claims, which include yet further distinguishing features of the

invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the claim amendments and arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330